**THE UNITED STATES DISTRICT COURT**
**FOR THE NORTHERN DISTRICT OF GEORGIA**

| | | |
|---|---|---|
| **JERRY TODD EVERHART, DEBORAH FRAZIER AND JOSEPH FRAZIER,** | ) | |
| **Plaintiffs,** | ) | **COMPLAINT** |
| **v.** | ) | **CLASS ACTION** |
| **COLONIAL PIPELINE COMPANY,** | ) | |
| **Defendant.** | ) | |

Plaintiffs, Jerry Todd Everhart, Deborah Frazier and Joseph Frazier ("Plaintiffs") bring this Class Action Complaint against Colonial Pipeline Company ("Colonial" or "Defendant"), individually and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

## I. INTRODUCTION

1. Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard personal identifiable information that Defendant obtained from the Plaintiffs and others under assurances of confidentiality, including without limitation, name, contact information, date of birth, government-issued ID (such as Social Security, military ID, tax ID, and driver's license numbers), and

health-related information (including health insurance information) (collectively, "personal identifiable information" or "PII"). Plaintiffs also allege Defendant failed to provide timely, accurate, and adequate notice to Plaintiffs and similarly situated individuals (collectively, "Class Members") that their PII had been lost and precisely what types of information was unencrypted and in the possession of unknown third parties.

2. According to its website and other public information, for decades, Defendant has owned and operated one of the largest pipeline companies in the world. The Colonial Pipeline is the largest pipeline system for refined oil products in the U.S. The pipeline itself is 5,500 miles long and can carry three million barrels of fuel per day between Texas and New York. It is operated by Colonial Pipeline Company, which is headquartered in Alpharetta, Georgia. A variety of stakeholders entrust Defendant with an extensive amount of their PII, including employees of Defendant, customers of Defendant, property owners who enter into transactions with Defendant as neighbors of the physical pipeline, individuals affected by legal proceedings with Defendant, and others who provide PII to the company as part of other commercial relationships. Defendant retains this information on computer hardware—even after the relevant transactions and relationships end. Defendant asserts that it understands the importance of protecting such information.

3. On May 7, 2021, Defendant learned that cybercriminals had staged a ransomware attack against Defendant's systems, which encrypted or "locked" certain data from use. While Defendant sought to efface the fact initially, the attack resulted in the exportation of voluminous data from those systems (the "Data Breach").

4. By the end of the day, Defendant paid the cybercriminals a $4.4 million ransom in return for a decryption tool that purportedly would allow Defendant to retrieve the encrypted or "locked" data after the Data Breach.

5. Even with the decryption tool, it took approximately five days for Defendant to restart the pipeline after the Data Breach.

6. The five-day shutdown of the pipeline resulted in fuel shortages in areas that the pipeline serviced, affecting more than 11,000 gas stations and causing a sharp increase in the price of gasoline for automobiles and other motor vehicles and a sharp decrease in convenience store sales.

7. In addition to shutting down the pipeline, the Data Breach allowed unauthorized access to files on Defendant's servers. These servers contained files that in turn contained information about stakeholders such as the Plaintiffs.

8. More than three months later, in a notice letter dated August 13, 2021, Defendant advised Plaintiffs of the Data Breach.

9. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendant admits that the unencrypted PII exposed to "unauthorized activity" included names, Social Security numbers, and dates of birth.

10. The exposed PII of Plaintiffs and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiffs and Class Members now face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers.

11. This PII was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the PII of Plaintiffs and Class Members. In addition to Defendant's failure to prevent the Data Breach, after discovering the breach, Defendant waited several months to report it to affected individuals. Defendant has also purposefully kept secret the specific vulnerabilities and root causes of the breach and has not informed Plaintiffs and Class Members of that information.

12. As a result of this delayed response, Plaintiffs and Class Members had no idea that their PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

13. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes and/or other law.

14. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include but are not limited to: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and (iv) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

15. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement

adequate and reasonable measures to ensure that the PII of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

## II. PARTIES

16. Plaintiff Jerry Todd Everhart resides at 393 Helmstetler Road, Lexington, North Carolina, Davidson County. Mr. Everhart received a letter from Defendant giving notice of a data breach, dated August 13, 2021 (the "August 13, 2021 Notice"), on or about that date. The notice stated that Plaintiff's "name, contact information, date of birth, government-issued ID (such as Social Security, military ID, tax ID, and driver's license numbers), and health-related information (including health insurance information)" may have been exposed.

17. Plaintiff Deborah Frazier resides at 350 Yarborough Drive, Lexington, North Carolina, Davidson County. Ms. Frazier received the August 13, 2021 Notice.

18. Plaintiff Joseph Frazier resides at 350 Yarborough Drive, Lexington, North Carolina, Davidson County. Mr. Frazier received the August 13, 2021 Notice.

19. Colonial is a Delaware and Virginia corporation and has a principal place of business in Alpharetta, Georgia. Its pipeline system originates in Houston, Texas and terminates in Linden, New Jersey. The pipeline transports refined petroleum products.

20. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiffs. Plaintiffs will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

21. All of Plaintiffs' claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

## III. JURISDICTION AND VENUE

22. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity.

23. The Northern District of Georgia has personal jurisdiction over the Defendant named in this action because Defendant and/or its parents or affiliates are

headquartered in this District and Defendant conduct substantial business in Georgia and this District through its headquarters, offices, parents, and affiliates.

24. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

## IV. FACTUAL ALLEGATIONS

***Background.***

25. Colonial was incorporated in 1961 and its pipeline system contains 5,500 miles of pipe, originates in Houston, Texas and terminates in Linden, New Jersey.

26. As of 2012, according to its Public & Government Affairs Manager, Colonial was the "[l]argest refined-products pipeline in the U.S." Colonial "delivers over 70% of the liquid fuel supply to GA, SC, NC, TN, and VA." Its pipeline system delivers "100 Million" gallons per day. Portions of its pipeline are located in Louisiana, Mississippi, Alabama, Georgia, Tennessee, South Carolina, North Carolina, Virginia, the District of Columbia, Maryland, and Pennsylvania. Colonial's pipeline carries millions of barrels of gasoline, diesel and jet fuel between the Gulf Coast and the New York Harbor area.

27. Over the pertinent times, Plaintiffs and similarly situated Class Members were required to provide Defendant with sensitive and confidential information, including names, Social Security numbers, dates of birth, and/or other personal identifiable information or PII, which is static, does not change, and can be used to commit myriad financial crimes.

28. Plaintiffs and Class Members relied on this sophisticated Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand security to safeguard their PII.

29. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiffs and Class Members from involuntary disclosure to third parties.

30. Defendant knew during the pertinent times that due to the nature of its business, it was periodically entrusted with the duty to safeguard the PII of myriad stakeholders. For example, employees and independent contractors relied on Colonial to protect their PII that they may have provided as part of an employment or insurance application. Customers may have provided PII as part of a business transaction. Property owners in areas where the pipeline ran, who entered into sales or leases of property where its pipeline passed or where its numerous booster stations and tank farms were located, or who entered into contract arrangements to allow Colonial to access the pipeline on their property, or to address environmental

matters, may have provided PII. Numerous other individuals may have provided Colonial with their PII and were fully justified in relying on the company to protect all their data.

31. On information and belief, Colonial is very well-resourced to invest in necessary infrastructure to safeguard against cyberhacking and ransomware-style attacks. Colonial, while privately held, is known to be owned by several of the largest energy companies in the world; its reported annual revenues are in excess of $500 million.

***The Data Breach.***

32. On May 7, 2021, Defendant learned that cybercriminals had performed the Data Breach which occurred in the form of a ransomware attack, thereby breaching and exfiltrating or stealing voluminous data of the company and encrypting data on Defendant's systems. In fact, as was subsequently learned, the threat actor who engaged in the attack had been on Defendant's computer system for a full week without detection, free to roam and copy materials. Defendant did not have a cybersecurity program encompassing ransomware issues in place at the time of this attack and Data Breach. As a result of the ransomware attack, Defendant elected to completely suspend operation of the Pipeline.

33. Many of the details of the root causes of the attack, the vulnerabilities exploited, and the remedial measures undertaken to ensure a similar attack does not

occur again have not been shared with the general public, Plaintiffs or Class Members, regardless of the harm the Data Breach has caused to them.

34. Analysis to date of the cyberattack on Colonial Pipeline has determined that hackers were able to access the company's network by using a compromised virtual private network ("VPN") password.

35. A VPN extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

36. Many companies prefer to use a VPN in addition to the private network found at their corporate offices. This is because by using the VPN, company employees can log in remotely from a physical location that is not at the company offices.

37. However, the use of a VPN brings with it obvious cybersecurity risks, because the individuals logging into the company's computer system are not restricted to simply those who are physically on site at the company offices.

38. To prevent disclosure of private information, VPNs typically allow only authenticated remote access using "tunneling" protocols and encryption techniques. Tunnel endpoints must be authenticated before secure VPN tunnels can be established. User-created remote-access VPNs may use passwords, biometrics, two-factor or multi-factor authentication or other cryptographic methods.

39. For networks with national security implications, and which provide essential infrastructure, such as the Defendant's pipeline, which Defendant itself admits in public pronouncements, it is grossly negligent to require nothing more by way of authentication than a simple login and password, on an outdated and superseded system, to access the inner workings of the company's system. Moreover it was grossly negligent for Defendant to allow a data breach including, on information and belief. unfettered access by the hackers to the sensitive and private data of Pipeline distributors, customers and users.

40. At some point in the past, Defendant switched from its old remote access system to one using two-factor or multi-factor authentication. However, when Defendant did so, it inexplicably left its old, less secure system intact and operational. Defendant took no steps to disable or eliminate the old system nor to eliminate the ability of departed employees – or bad actors who have stolen employee credentials – to access it undetected.

41. The ransomware attack actors who committed the Data Breach herein gained access to the company's computer networks by using a compromised employee password.

42. The password had been linked to Defendant's disused VPN account for remote access. This account was not guarded by an extra layer of security via multi-

factor authentication. There was no mechanism, for example, for use of a one-time password to ensure security.[1]

43. Stated differently, the password was associated with an outdated "legacy" VPN platform. The platform had been replaced by the company's newer system using multi-factor authentication using RSA tokens.[2] For whatever reason, when Defendant put up its new platform, it neglected to take down its old one, imperiling the security of both.

44. The hackers had apparently found the password from data on the dark web. The login and password were outdated in that they were no longer used by any employees, but they were still valid in the Colonial Pipeline network and allowed the attackers to enter the network on April 29, 2021. The employee who had used the login and password on Colonial's old system had apparently also used it on another website that got hacked.

45. After entering the system, the attackers explored the Colonial Pipeline computer system for approximately a week, wholly undetected, before sending the ransom note and activating the ransomware.

---

[1] Prepared Statement of Charles Carmakal, Senior Vice President and Chief Technology Officer, FireEye-Mandiant, before the United States House Committee on Homeland Security, June 9, 2021 ("The earliest evidence of compromise that we have identified to date occurred on April 29, 2021. On that date, the threat actor had logged into a virtual private network (VPN) appliance using a legacy VPN profile and an employee's username and password. The legacy VPN profile did not require a one-time passcode to be provided. The legacy VPN profile has since been disabled as part of Colonial Pipeline's remediation process.").

[2] RSA tokens are part of a remote-access security system offered by RSA Security.

46. Colonial's computer system includes voluminous information related to the intricate web of gas and oil product suppliers and customers, property owners affected by the vast pipeline network, employees who worked a myriad of job duties along the pipeline, in its tank farms or booster stations, or at its administrative and control center offices, and others. This information is used by Colonial for billing and commercial purposes and the company possesses voluminous private and sensitive information regarding these stakeholders. When they provide sensitive and private billing, accounting and financial information to Colonial, they do so under an expectation that the company will keep the information private and take reasonable steps to safeguard the information.

47. When the breach first occurred on April 29, 2021, it was not discovered. After the hackers had reviewed and stolen or exfiltrated data for a week, they then used software to encrypt or disable some of the billing and other systems on Defendant's computer system. This encryption however did not extend to include Defendant's separately siloed pipeline control systems. However, Defendant lacked either the trained management or the action plan to promptly assess the ransomware once installed. The threat actor put up the electronic ransomware note on the Colonial computer system which was discovered at or about 5 a.m. on May 7, 2021 by a control room employee in the Alpharetta, Georgia headquarters. He brought

the matter to his supervisor in the control room. According to Defendant, the company decided to shut down the pipeline at about 6 a.m.

48. As noted, the login and password that the attackers used were for the remote access account of an inactive employee. Even though the employee had left Colonial Pipeline, Defendant allowed the account to remain active. When an employee leaves a company, the proper practice is to shut down their login and password. However, Defendant neither did that, nor had in place an effective audit system to check and make sure accounts of departed employees could not be used, nor did Defendant take steps to ensure the old remote access system was shut down once a new system was acquired.

49. FBI and government guidance states that those receiving ransom demands from ransomware attackers should not pay the ransom. However, by the end of May 7 Defendant elected to negotiate with the hackers and pay the ransom on May 8. Defendant has since stated that it has cybersecurity insurance that it expects will cover the entire amount of the ransom loss.

***Additional Facts on Defendant's Failure to Use Proper Procedures.***

50. Defendant did not use reasonable security procedures and practices appropriate to operating the largest pipeline system in the United States for refined petroleum products in the time period leading up to the attack.

51. As explained by the FBI, "[p]revention is the most effective defense

against ransomware and it is critical to take precautions for protection."[3]

52. To prevent and detect ransomware attacks, including the one that occurred here, Defendant could and should have implemented the following measures:

- Implement an awareness and training program, so stakeholders and those at the company itself can be aware of the threat of ransomware and how it is delivered.
- Educate top management on ransomware and similar cybersecurity threats and designate an executive management position to handle cybersecurity issues.
- Ensure that old VPN remote access systems are taken down when new ones are instituted.
- Ensure that employee logins and passwords that are no longer being used are turned off and disabled.
- Allow government agencies charged with the mission of assisting private industry to ensure their adequate cybersecurity are given recognition and cooperation, rather than rejecting their efforts to assist.
- Ensure that when it comes to a private company that holds an effective monopoly and a bottleneck over critical infrastructure with national security implications, that company does not use VPN remote access with lax security measures.
- Require two-factor or multi-factor authentication for any and all remote access to the company's computer systems.
- Ensure regular, thorough cybersecurity audits.
- Engage outside cybersecurity consultants and firms to ensure industry standards are met for cybersecurity for the company.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent

[3] *See* Ransomware Prevention and Response for Chief Information Security Officers, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/ LocalAppData folder.
- Disable Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[4]

53. To prevent and detect ransomware attacks, including the Data Breach

[4] *Id.* at 3-4.

and ransomware attack herein, Defendant could have, and should have, implemented the following measures recommended by the Microsoft Threat Protection Intelligence Team, in addition to the measures alleged elsewhere herein:

**Secure internet-facing assets**

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

**Thoroughly investigate and remediate alerts**

- Prioritize and treat commodity malware infections as potential full compromise;

**Include IT Pros in security discussions**

- Ensure collaboration among security operations, security admins, and information technology admins to configure servers and other endpoints securely;

**Build credential hygiene**

- Use multi-factor authentication or network level authentication and use strong, randomized, just-in-time local admin passwords

**Apply principle of least-privilege**

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

**Harden infrastructure**

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection

- Turn on attack surface reduction rules and Antimalware Scan Interface for Office [Visual Basic for Applications].[5]

54. Given that Defendant was operating the largest pipeline system in the United States for refined petroleum products, Defendant could and should have implemented all of the above measures to prevent and detect ransomware attacks.

55. The occurrence of the ransomware attack indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach that impacted numerous affected individuals, including Plaintiffs and Class Members.

56. Defendant's failure to detect and prevent the attack was compounded by its unreasonable refusal, both before and after the ransomware attack, to participate in security assessments.

57. It was reported on June 15, 2021, that the Transportation Security Administration ("TSA") "prior to the attack asked Colonial Pipeline on no less than thirteen occasions to participate in physical and cyber pipeline security assessments. Citing COVID-19, Colonial repeatedly delayed and chose not to participate. On multiple occasions, Colonial didn't even bother responding to TSA's emails. In fact, Colonial still has not agreed to participate in the physical assessment, and only

[5] Adapted from Microsoft 365 Defender Threat Intelligence Team, Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

agreed to cooperate with TSA's cybersecurity assessment three weeks after the ransomware attack occurred."[6]

58. Colonial's unreasonable refusal to participate in cyber pipeline security assessments reflected deliberate indifference to its obvious and well-established duty to Plaintiffs and Class Members: "when you operate infrastructure that we all depend on, you have a responsibility to the public."[7]

59. Defendant's shutdown of the pipeline was a sudden calamitous event that jeopardized the security and livelihoods of those who depend upon ready access to gasoline for a variety of uses and reasons.

60. Defendant halted the pipeline on May 7, 2021. The pipeline remained shut down on May 8, May 9, May 10 and May 11. The restart of pipeline operations did not begin until 5 p.m. on May 12, ending a six-day shutdown. However, even then, it took time thereafter for service to return to normal.

61. On or about August 13, 2021, Defendant sent Plaintiffs the August 13, 2021 Notice. Defendant informed Plaintiffs that: "As you are aware, Colonial Pipeline Company recently experienced a cybersecurity incident. Promptly after learning of the issue, we took steps to understand its nature and scope and to secure

[6] Committee on Homeland Security, Joint Hearing Statement of Transportation & Maritime Security Subcommittee Chairwoman Bonnie Watson Coleman (D-NJ), *Cyber Threats in the Pipeline: Lessons from the Federal Response to the Colonial Pipeline Ransomware Attack*, at 1 (June 15, 2021).
[7] *Id.* at 2.

our systems. We engaged leading outside security experts to assist with our investigation and have implemented additional information security measures to enhance our safeguards. We also coordinated with law enforcement…."

62. Defendant admitted in the August 13, 2021 Notice that unauthorized third persons had accessed files that contained sensitive information, including name, contact information, date of birth, government-issued ID (such as Social Security, military ID, tax ID, and driver's license numbers), and/or health-related information (including health insurance information.

63. The unencrypted PII of Plaintiffs and Class Members may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

64. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiffs and Class Members, causing the exposure of PII for numerous individuals.

65. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[8]

66. Given that Defendant was storing the PII of numerous individuals, collected over years, Defendant could and should have implemented any and all necessary measures to prevent and detect ransomware attacks.

67. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the relevant measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII of numerous individuals, including Plaintiffs and Class Members.

***Defendant Acquires, Collects, and Stores the PII.***

68. Defendant acquired, collected, and stored the PII of Plaintiff and Class Members over a period of years.

69. As a condition of agreeing to contracts or entering into other business arrangements with Defendant, or functioning as a customer of Defendant, Defendant requires that Plaintiffs and Class Members entrust Defendant with highly confidential PII.

[8] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

70. By obtaining, collecting, and storing the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

71. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

***Securing PII and Preventing Breaches.***

72. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiffs and Class Members, or through other steps.

73. Defendant's negligence in safeguarding the PII of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

74. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

75. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201 (2013).

76. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

77. The ramifications of Defendant's failure to keep secure the PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

***Value of Personal Identifiable Information.***

78. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200. Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web. Criminals can also purchase access to entire company data breaches from $900 to $4,500.

79. Social Security numbers are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses

and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud: "A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems."

80. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

81. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number,

so all of that old bad information is quickly inherited into the new Social Security number."

82. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number, driver's license number, name, and date of birth.

83. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."

84. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

85. The fraudulent activity resulting from the Data Breach may not come to light for years.

86. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study

regarding data breaches: "[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."

87. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

88. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

89. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's file servers, amounting to potentially tens or hundreds of thousands of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

90. To date, Defendant has offered Plaintiffs and Class Members only limited monitoring services through a single credit bureau, Experian. The offered service is inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

91. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

***Plaintiffs' Experience.***

92. For years, Plaintiff Mr. Everhart has owned property and has resided in the vicinity of Defendant's pipeline. Within the last several years, he was obligated to provide his PII to Defendant in connection with property rights and environmental matters having to do with Defendant's pipeline. Specifically, Defendant had contaminated a significant area of property adjacent to its pipeline infrastructure.

93. Plaintiffs Mr. and Mrs. Frazier likewise have owned property and have resided in the vicinity of Defendant's pipeline. Like Mr. Everhart, they were obligated to provide their PII to Defendant in connection with property rights and environmental matters having to do with Defendant's pipeline.

94. Mr. Everhart and Mr. and Mrs. Frazier all received the August 13, 2021 Notice, dated August 13, 2021, on or about that date.

95. As a result of the August 13, 2021 Notice, Mr. Everhart and Mr. and Mrs. Frazier each have spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the August 13, 2021 Notice, exploring credit monitoring and identity theft insurance options, signing up for and monitoring the credit monitoring offered by Defendant, and/or self-monitoring their accounts. This time has been lost forever and cannot be recaptured.

96. Additionally, Mr. Everhart and Mr. and Mrs. Frazier are very careful about sharing their PII. They have never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

97. Each Plaintiff stores any documents containing his or her PII in a safe and secure location or destroys the documents. Moreover, each diligently chooses unique usernames and passwords for their various online accounts.

98. Each Plaintiff suffered actual injury in the form of damages to and diminution in the value of his or her PII—a form of intangible property that each entrusted to Defendant, which was compromised in and as a result of the Data Breach.

99. Each Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his or her privacy.

100. Each Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his or her PII, especially his or her Social Security number, in combination with name and date of birth, being placed in the hands of unauthorized third parties and possibly criminals.

101. Each Plaintiff has a continuing interest in ensuring that his or her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

***Defendant Knew or Should Have Known of the Dangers.***

102. In the years and months leading up to May 7, 2021, the dangers of ransomware attacks and data breaches had become well-known among IT professionals and computer systems managers at large corporations such as Defendant. Defendant was well-aware of the quantity of critical and commercially sensitive information in its computer systems. And Defendant is a massively resourced company owned by some of the largest gas and oil interests in the world. However, Defendant had failed to take reasonable steps to secure and protect its systems against data breach and ransomware attacks.

103. Ransomware attacks have been known to occur for years. Furthermore, in the months leading up to May 7, 2021, the number and scope of ransomware attacks had expanded, and this fact was known to those in the IT industry.

104. Defendant's own retained consultant, Mandiant, described after the instant attack that "[i]n 2015, Mandiant observed a notable surge in disruptive intrusions in which threat actors deliberately destroyed critical business systems, leaked confidential data, taunted executives, and extorted organizations."[9]

105. "The problem has steadily grown worse in recent years, and in 2020, nearly 2,400 U.S.-based governments, healthcare facilities, and schools were victims of ransomware, according to the security firm Emsisoft."[10]

106. In addition, for years, it had been known and publicized that critical infrastructure such as pipelines were especially vulnerable to the assaults of both conventional and cyber-criminals, and that therefore investing adequately in cyber-security was essential for those who desired to be in the pipeline business.

107. Pipelines in the United States have been the target of several confirmed terrorist plots and attempted physical attacks since September 11, 2001.[11]

108. In 2011, the computer security company McAfee reported "coordinated covert and targeted" cyberattacks originating primarily in China against global

[9] Prepared Statement of Charles Carmakal, Senior Vice President and Chief Technology Officer, FireEye-Mandiant, before the United States House Committee on Homeland Security, June 9, 2021.
[10] Ransomware Task Force, Institute for Security and Technology, Combating Ransomware, A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force, p. 7, https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf.
[11] Paul W. Parfomak, Pipeline Cybersecurity: Federal Policy, Aug. 16, 2012, Congressional Research Service.

energy companies. The attacks began in 2009 and involved a hacking tactic known as "spear-phishing," exploitation of Microsoft software vulnerabilities, and the use of remote administration tools to collect sensitive competitive information about oil and gas fields.[12]

109. In 2012, authorities warned that changes to pipeline computer networks over the years, the emergence of more sophisticated hackers, and the development of specialized malicious software had made pipeline supervisory control and data acquisition operations increasingly vulnerable to cyberattacks.[13]

110. In 2011-12, there were a coordinated series of cyber intrusions specifically targeting U.S. pipeline computer systems.[14] From December 2011 through June 2012, cyberspies linked to China's military targeted nearly two dozen U.S. natural gas pipeline operators. The attack targeted 23 gas pipeline companies, according to information from the Department of Homeland Security ("DHS") and the DHS's Industrial Control Systems Cyber Emergency Response Team ("ICS-CERT").[15]

---

[12] Prepared Statement of Paul W. Parfomak, April 19, 2016, to the U.S. House of Representatives, Committee on Homeland Security, Subcommittee on Transportation Security, April 19, 2016.
[13] *Id.*
[14] *Id.*
[15] Mark Clayton, Exclusive: Cyberattack leaves natural gas pipelines vulnerable to sabotage, Christian Science Monitor, February 27, 2013; Kevin E. Hemsley and Dr. Ronald E. Fisher, History of Industrial Control System Cyber Incidents, Dec. 2018, INL/CON-18-44411-Revision-2, p. 10; Gas Pipeline Cyber Intrusion Campaign – Update, ICS/CERT Monthly Monitor, June-July 2012.

111. After the 2011-12 attacks occurred, ICS-CERT broadly disseminated information about the attacks to asset owners and operators.[16] On information and belief this included dissemination to representatives of Defendant.

112. In 2013, ICS-CERT, in coordination with the FBI, the U.S. Department of Energy ("DOE"), the Electricity Sector Information Sharing and Analysis Center ("ES-ISAC"), the TSA, and the Oil and Natural Gas and Pipelines Sector Coordinating Councils Cybersecurity Working Group, conducted a series of 14 action campaign briefings in response to the growing number of cyber-incidents related to U.S. critical infrastructure. The briefings were given to over 750 attendees in cities throughout the country to assist critical infrastructure asset owners and operators in detecting intrusions and developing mitigation strategies.[17] On information and belief, Defendant's representatives attended these briefings.

113. In 2013, congressional hearings were held on the subject of critical infrastructure and cyber threats. Those who testified at these hearings noted, among other things, that "pipeline networks … are susceptible … to internet-delivered attacks."[18]

---

[16] *Id.*
[17] *Id.*
[18] Statement of Dean Picciotti, Cyber Threats from China, Russia, and Iran: Protecting American Critical Infrastructure, hearing before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, of the Committee on Homeland Security, House of Representatives, 113th Congress, First Session, March 20, 2013.

114. In a campaign lasting from early 2013 through 2014, an allegedly Russia-backed group known as Dragonfly or Energetic Bear targeted electricity distribution, electricity generation, oil pipeline and energy industry industrial equipment manufacturers via supply chain cyberattacks.[19]

115. In 2016, during further congressional hearings, speakers noted the need to "thwart malicious actors with ill intentions from damaging or disrupting pipeline operations" and that "[i]n addition to physical attacks, we must also guard against cyber attacks." The speakers noted that "adversaries … have shown a proclivity for launching sophisticated cyber attacks against U.S. companies, banks, and critical infrastructure." There had been "several high-profile incidents where the systems of global energy companies have been compromised and sensitive information fell into the wrong hands."[20] Speakers discussed "pipeline data security," and techniques for "pipeline operators defend their systems from cyber attacks,"[21] and noted that "cybersecurity threats to pipelines have been increasing."[22] The President of the

[19] Booz Allen, Industrial Cybersecurity Threat Briefing, 2016, p. 15; Kevin E. Hemsley and Dr. Ronald E. Fisher, History of Industrial Control System Cyber Incidents, Dec. 2018, INL/CON-18-44411-Revision-2, p. 3.
[20] Statement of Hon. John Katko, Chairman, U.S. House of Representatives, Committee on Homeland Security, Subcommittee on Transportation Security, hearing entitled Pipelines: securing the veins of the American economy, April 19, 2016.
[21] Statement of Andrew J. Black, President and CEO, Association of Oil Pipe Lines, to the U.S. House of Representatives, Committee on Homeland Security, Subcommittee on Transportation Security, April 19, 2016.
[22] Prepared Statement of Paul W. Parfomak, April 19, 2016, to the U.S. House of Representatives, Committee on Homeland Security, Subcommittee on Transportation Security, April 19, 2016.

Association of Oil Pipe Lines promised that the pipeline industry was focused on "being prepared for cyber attacks."[23]

116. In a 2017 report, the Congressional Research Service described that "[w]hile physical threats to the U.S. power grid and pipelines have long worried policymakers, cyber threats to the computer systems that operate this critical infrastructure are an increasing concern."[24] The report found that the "secure operation of both the power grid and pipelines are national priorities and that "the electricity grid and energy pipelines are under the same types of cybersecurity risks as other industries, such as financial services or transportation."[25]

117. In January 2019, the Director of National Intelligence in a statement for the record described that "China has the ability to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks—in the United States."[26]

118. An August 2019 GAO report described that "nation-state, state-sponsored, and state-sanctioned groups or programs, use cyber tools as part of their information-gathering and espionage activities." The report noted that "China and

[23] Congressional Research Service, Cybersecurity for Energy Delivery Systems: DOE Programs, August 28, 2017, executive summary.
[24] *Id.*
[25] *Id.*, pp. 1-2.
[26] Daniel R. Coats, Director of National Intelligence, Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, p. 5, Jan. 29, 2019, Senate Select Committee on Intelligence, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

Russia pose the greatest cyberattack threats" with "the ability to disrupt a natural gas pipeline for days to weeks."[27]

119. In February 2020, a ransomware attack on a natural-gas pipeline operator halted operations for two days.[28] The alert from the Cybersecurity and Infrastructure Security Agency ("CISA") described a ransomware attack on an unnamed natural-gas pipeline operator that halted operations for two days while staff shut down, then restored, systems. The alert said that although staff did not lose control of operations, the company did not have a plan in place for responding to a cyberattack.

120. In the weeks and months leading up to the Ransomware Attack on May 7, 2021, Defendant rejected offers by government agencies to assess its cyber security defenses. In hearings occurring after the attack, speakers were "troubled by reports that Colonial declined repeated offers by TSA over the past year to assess its security defenses."[29]

121. TSA's Critical Facility Security Review ("CFSR") examines and provides security recommendations on pipeline facilities, while the Validated

[27] GAO, Report to Congressional Requesters, Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid, August 2019, GAO-19-332, p. 17 https://www.gao.gov/assets/gao-19-332.pdf
[28] Ransomware Task Force, Combating Ransomware, *supra*, p. 8.
[29] Hearing Statement of Chairman Bennie G. Thompson (D-MS), for hearing on Cyber Threats in the Pipeline: Using Lessons from the Colonial Ransomware Attack to Defend Critical Infrastructure, June 9, 2021.

Architecture Design Review ("VADR") assesses cybersecurity and has been available in virtual format at least since July 2020. However, in hearings occurring after the Ransomware Attack, Defendant's CEO Joseph Blount admitted that Defendant had failed to agree to work and meet with the TSA in that regard in the months leading up to the attack.[30]

122. Those hearings also revealed that as noted above, in the weeks and months leading up to the Ransomware Attack, Defendant had an old log in system it forgot to shut down. This old system allowed remote access without the safety of double authentication measures that have been offered by software companies for years. Despite its special duty to use safety measures due to its role in national security and essential infrastructure, Defendant had failed to ensure that those seeking remote access could not log in except by multi-factor authentication so as to make sure the person using the computer was who he or she claimed to be. Because Colonial had left up a system that did not use multi-factor authentication, this allowed the hackers to access its network with a compromised username and password.

[30] Jule Pattison-Gordon, US House Interrogates Colonial Pipeline CEO Joseph Blount, June 10, 2021, Government Technology, https://www.govtech.com/security/us-house-interrogates-colonial-pipeline-ceo-joseph-blount?_amp=true.

123. During the pertinent times, Defendant engaged in rudimentary cybersecurity failures and did not even have a Chief Information Security Officer.[31] The manner in which the breach occurred, by use of stolen credentials, was consistent with the number one vector for data breaches in 2019.[32]

124. Under the facts and circumstances, Defendant was aware of a substantial cyber security risk dating back for years but failed to implement reasonable security measures to combat it.[33]

## V. CLASS ALLEGATIONS

125. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

126. The Nationwide Class that Plaintiffs seek to represent is defined as follows: All individuals whose PII was compromised in the data breach that is the

[31] Colonial Pipeline hackers gained access via unprotected VPN account: password leaked, no MFA, The Stack (describing "rudimentary cyber hygiene failures at the pipeline company, which did not have a Chief Information Security Officer"), https://thestack.technology/how-the-colonial-pipeline-hack-happened/.

[32] *Id.* ("Stolen credentials were the number one vector for data breaches in 2019, according to this Verizon Data Breach report.").

[33] Lawmakers Chide Colonial Pipeline for Weak Cybersecurity, June 9, 2021, Bloomberg News ("'If your pipeline provides fuel to 45% of the East Coast, why are you only hardening systems after an attack? Why wasn't it done beforehand?' said Rep. John Katko (R-N.Y.), ranking member of the House Homeland Security Committee, which held a hearing June 9 on lessons learned from the attack."). At https://www.ttnews.com/articles/lawmakers-chide-colonial-pipeline-weak-cybersecurity.

subject of the August 13, 2021 Notice that Defendant sent to Plaintiffs on or around August 13, 2021 (the "Nationwide Class").

127. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiffs assert claims on behalf of a separate subclass, defined as follows: All current and former contracting parties in contracts with Defendant who had contracts related to PII that was compromised in the data breach that is the subject of the August 13, 2021 Notice that Defendant sent to Plaintiffs on or around August 13, 2021 (the "Contract Class").

128. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

129. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

130. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide Class (the "Class") are so numerous that joinder of all members is impracticable. Numerous

individuals, and beneficiaries and dependents thereof, exist whose PII may have been improperly accessed in the Data Breach, and the Class is apparently identifiable within Defendant's records.

131. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

A. Whether and to what extent Defendant had a duty to protect the PII of Plaintiffs and Class Members;
B. Whether Defendant had duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;
C. Whether Defendant had duties not to use the PII of Plaintiffs and Class Members for non-business purposes;
D. Whether Defendant failed to adequately safeguard the PII of Plaintiffs and Class Members;
E. Whether and when Defendant actually learned of the Data Breach;
F. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;
G. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their PII had been compromised;
H. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
I. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
J. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members;
K. Whether Plaintiffs and Class Members are entitled to actual damages, consequential damages, and/or nominal damages as a result of Defendant's wrongful conduct;

L. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

M. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

132. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance.

133. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

134. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel

experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

135. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

136. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs

of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which each Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

137. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

138. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

139. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

140. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

141. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

A. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;
B. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;
C. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
D. Whether a contract existed between Defendant on the one hand, and Plaintiffs and Class Members on the other, and the terms of that contract;
E. Whether Defendant breached the implied contract;
F. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their PII had been compromised;
G. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
H. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members; and,
I. Whether Class Members are entitled to actual damages, consequential damages, nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

**COUNT I**
**NEGLIGENCE**
**(On Behalf of Plaintiffs and the Nationwide Class)**

142. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 141.

143. As a condition of their agreements and arrangements with Defendant, Plaintiffs and Class Members were obligated to provide Defendant with certain PII, including their names, Social Security numbers, dates of birth, and/or other PII.

144. Plaintiffs and the Nationwide Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

145. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Nationwide Class could and would suffer if the PII were wrongfully disclosed.

146. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiffs and the Nationwide Class involved an unreasonable risk of harm to Plaintiffs and the Nationwide Class, even if the harm occurred through the criminal acts of a third party.

147. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII of Plaintiffs and the Nationwide Class in Defendant's possession was adequately secured and protected.

148. Defendant also had a duty to exercise appropriate clearinghouse practices to remove individuals' PII, it was no longer required to retain pursuant to regulations.

149. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiffs and the Nationwide Class.

150. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and the Nationwide Class. That special relationship arose because Plaintiffs and the Nationwide Class entrusted Defendant with their confidential PII, a necessary part of their transaction with the company.

151. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or the Nationwide Class.

152. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Nationwide Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

153. Plaintiffs and the Nationwide Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Nationwide Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

154. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and the Nationwide Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the PII of Plaintiffs and the Nationwide Class, including basic encryption techniques freely available to Defendant.

155. Plaintiffs and the Nationwide Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

156. Defendant was in a position to protect against the harm suffered by Plaintiffs and the Nationwide Class as a result of the Data Breach.

157. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiffs and the Nationwide Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Nationwide Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

158. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiffs and the Nationwide Class.

159. Defendant has admitted that the PII of Plaintiffs and the Nationwide Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

160. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and the Nationwide Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiffs and the Nationwide Class during the time the PII was within Defendant's possession or control.

161. Defendant improperly and inadequately safeguarded the PII of Plaintiffs and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

162. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiffs and the Nationwide Class in the face of increased risk of theft.

163. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and the Nationwide Class by failing to have appropriate procedures in place to detect and prevent dissemination of PII.

164. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove PII when it was no longer required to be retained pursuant to regulations.

165. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiffs and the Nationwide Class the existence and scope of the Data Breach.

166. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Nationwide Class, the PII of Plaintiffs and the Nationwide Class would not have been compromised.

167. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiffs and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Nationwide Class. The PII of Plaintiffs and the Nationwide Class was lost and accessed as the

proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

168. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

169. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the harm that would result to Plaintiffs and the Nationwide Class.

170. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

171. Plaintiffs and the Nationwide Class are within the class of persons that the FTC Act was intended to protect.

172. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable

data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Nationwide Class.

173. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiffs and the Nationwide Class; and (viii) present and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Nationwide Class.

174. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

175. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and the Nationwide Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

## COUNT II
## BREACH OF CONTRACT
## (On Behalf of Plaintiffs and the Contract Class)

176. Plaintiffs and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 175.

177. Defendant required Plaintiffs and the Contract Class to provide their personal information, including names, Social Security numbers, and dates of birth, and/or other PII, as a condition of a contract.

178. As a condition of their contracts with Defendant, Plaintiffs and the Contract Class provided their personal and financial information. In so doing,

Plaintiffs and the Contract Class entered into express or implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Contract Class if their data had been breached and compromised or stolen.

179. Plaintiffs and the Contract Class fully performed their obligations under the contracts with Defendant.

180. Defendant breached the contracts it made with Plaintiffs and the Contract Class by failing to safeguard and protect their personal and financial information, and by failing to provide timely and accurate notice to them that personal and financial information was compromised as a result of the Data Breach.

181. As a direct and proximate result of Defendant's above-described breach of contract, Plaintiffs and the Contract Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and

credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

## COUNT III
## INVASION OF PRIVACY
## (On Behalf of Plaintiffs and the Nationwide Class)

182. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 181.

183. Plaintiffs and the Nationwide Class had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

184. Defendant owed a duty to Plaintiffs and the Nationwide Class to keep their PII contained as a part thereof, confidential.

185. Defendant failed to protect and released to unknown and unauthorized third parties the PII of Plaintiffs and the Nationwide Class.

186. Defendant allowed unauthorized and unknown third parties access to and examination of the PII of Plaintiffs and the Nationwide Class, by way of Defendant's failure to protect the PII.

187. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiffs and the Nationwide Class is highly offensive to a reasonable person.

188. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and the Nationwide Class disclosed their PII to Defendant as part of their relationship with Defendant, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and the Nationwide Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

189. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiffs' and the Nationwide Class's interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

190. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

191. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and the Nationwide Class.

192. As a proximate result of the above acts and omissions of Defendant, the PII of Plaintiffs and the Nationwide Class was disclosed to third parties without authorization, causing Plaintiffs and the Nationwide Class to suffer damages.

193. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Nationwide Class in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiffs and the Nationwide Class have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Nationwide Class.

## COUNT IV
## BREACH OF CONFIDENCE
## (On Behalf of Plaintiffs and the Nationwide Class)

194. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 193.

195. At all times during Plaintiffs' and the Nationwide Class's interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiffs' and the Nationwide Class's PII that Plaintiffs and the Nationwide Class provided to Defendant.

196. As alleged herein and above, Defendant's relationship with Plaintiffs and the Nationwide Class was governed by terms and expectations that Plaintiff's and the Nationwide Class's PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

197. Plaintiffs and the Nationwide Class provided Plaintiffs' and the Nationwide Class's PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII to be disseminated to any unauthorized third parties.

198. Plaintiffs and the Nationwide Class also provided Plaintiffs' and the Nationwide Class's PII to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that PII from unauthorized disclosure.

199. Defendant voluntarily received in confidence Plaintiffs' and the Nationwide Class's PII with the understanding that PII would not be disclosed or disseminated to the public or any unauthorized third parties.

200. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiffs and the Nationwide Class's PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and the Nationwide Class's confidence, and without their express permission.

201. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiffs and the Nationwide Class have suffered damages.

202. But for Defendant's disclosure of Plaintiffs' and the Nationwide Class's PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties.

Defendant's Data Breach was the direct and legal cause of the theft of Plaintiffs' and the Nationwide Class's PII as well as the resulting damages.

203. The injury and harm Plaintiffs and the Nationwide Class suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and the Nationwide Class's PII. Defendant knew or should have known its methods of accepting and securing Plaintiffs' and the Nationwide Class's PII was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiffs' and the Nationwide Class's PII.

204. As a direct and proximate result of Defendant's breach of its confidence with Plaintiffs and the Nationwide Class, Plaintiffs and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject

to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII; and (viii) present and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Nationwide Class.

205. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

## PRAYER FOR RELIEF

**WHEREFORE**, Plaintiffs, on behalf of themselves and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class and the Contract Class and appointing Plaintiffs and their Counsel to represent each such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiffs and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

   i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xii. requiring Defendant to routinely and continually conduct internal

training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

## DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: August 27, 2021.

/s/ *Gregory John Bosseler*

Gregory John Bosseler
SBN 742496
MORGAN & MORGAN, PLLC
191 Peachtree St., NE
Suite 4200
Atlanta, GA 30306
Phone: (239) 433-6880
gbosseler@forthepeople.com

John A. Yanchunis*
Ryan D. Maxey*
MORGAN & MORGAN COMPLEX BUSINESS DIVISION
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Phone: (813) 223-5505
jyanchunis@ForThePeople.com
rmaxey@ForThePeople.com

Joel R. Rhine*
NC State Bar No. 16028
Martin Ramey*
NC State Bar No. 33617
Janet Coleman*
NC State Bar No. 12363
Ruth Sheehan*
NC State Bar No. 48069
RHINE LAW FIRM, P.C.
1612 Military Cutoff Rd., Suite 300
Wilmington, N.C. 28403
Office: (910) 772-9960
Cell: (910) 512-7888
jrr@rhinelawfirm.com
mjr@rhinelawfirm.com
jrc@rhinelawfirm.com
ras@rhinelawfirm.com

Mona Lisa Wallace*
NC State Bar No. 9021
John S. Hughes*
NC State Bar No. 22126
WALLACE AND GRAHAM, P.A.
525 North Main Street
Salisbury, NC 28144
Phone: (704) 633-5244
Fax: (704) 633-9434
mwallace@wallacegraham.com
jhughes@wallacegraham.com

**pro hac vice to be filed*

*Attorneys for Plaintiff*